PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 16 March 2000 (16.03.00)	
International application No.: PCT/SG98/00067	Applicant's or agent's file reference: FP1059
International filing date: 07 September 1998 (07.09.98)	Priority date:
Applicant: WU, Jian, Kang et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International preliminary Examining Authority on:

   09 February 2000 (09.02.00)

   [ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FP1059	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/SG 98/00067	International filing date *(day/month/year)* 7 September 1998 (07.09.1998)	Priority Date *(day/month/year)*

International Patent Classification (IPC) or national classification and IPC

IPC⁷: G09K 9/00, G07C 9/00

IPC^7: G09K 9/00, G07C 9/00

Applicant

Kent Ridge Digital Labs et al.

1. This international preliminary examination report has been prepared by this International Preliminary Examination Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of ___4___ sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

   I.   ☒ Basis of the opinion

   II. ☐ Priority

   III. ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   IV. ☒ Lack of unity of invention

   V.   ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI. ☐ Certain documents cited

   VII. ☐ Certain defects in the international application

   VIII. ☐ Certain observations on the international application

Date of submission of the demand 9 February 2000 (09.02.2000)	Date of completion of this report 29 March 2001 (29.03.2001)
Name and mailing address of the IPEA/AT **Austrian Patent Office** Kohlmarkt 8-10 A-1014 Vienna Facsimile No. 1/53424/200	Authorized officer SCHLECHTER Telephone No. 1/53424/448

Form PCT/IPEA/409 (cover sheet) (July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/SG 98/00067

I.	**Basis of the report**

1. With regard to the **elements of the international application:***

    ☒ the international application as originally filed

    ☐ the description:
    pages _____ , as originally filed
    pages _____ , filed with the demand
    pages _____ , filed with the letter of _____ .

    ☐ the claims:
    pages _____ , as originally filed
    pages _____ , as amended (together with any statement) under Article 19
    pages _____ , filed with the demand
    pages _____ , filed with the letter of _____ .

    ☐ the drawings:
    pages _____ , as originally filed
    pages _____ , filed with the demand
    pages _____ , filed with the letter of _____ .

    ☐ the sequence listing part of the description:
    pages _____ , as originally filed
    pages _____ , filed with the demand
    pages _____ , filed with the letter of _____ .

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

    ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

    ☐ the language of publication of the international application (under Rule 48.3(b)).

    ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/ or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

    ☐ contained in the international application in printed form.

    ☐ filed together with the international application in computer readable form.

    ☐ furnished subsequently to this Authority in written form.

    ☐ furnished subsequently to this Authority in computer readable form.

    ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

    ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

    ☐ the description, pages _____ .

    ☐ the claims, Nos. _____ .

    ☐ the drawings, sheets/fig _____ .

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as „originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

Form PCT/IPEA/409 (Box I) (July 1998))

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

    ☐ restricted the claims.

    ☐ paid additional fees.

    ☐ paid additional fees under protest.

    ☐ neither restricted nor paid additional fees.

2. ☐ This Authority found that the requirements of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirements of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

    ☐ complied with.

    ☒ not complied with for the following reasons:

Claims 1-27: Method of generating a key and/or access controls person's biometric data.
Claim 28: Codebook for storing data.

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this opinion:

    ☐ all parts.

    ☒ the parts relating to claims Nos. 1-27 .

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	3,9-11	YES
	Claims	1,2,4-8,12-27	NO
Inventive step (IS)	Claims		YES
	Claims	1-27	NO
Industrial applicability (IA)	Claims	1-27	YES
	Claims		NO

Citations and explanations (Rule 70.7)

The following documents are cited in the Search Report:

D1: DE 4243908 A1
D2: WO 9608093 A1
D3: US 5497430 A

Though the International Search Report in context with the Written Opinion transmitted to the Applicant raised objections with respect to novelty of claims 1, 2, 4 to 8 and 12 to 27 as well as inventiveness with regard to claims 3 and 9 to 11 of the present application, no amendments have been submitted.

Therefore, the missing novelty respectively inventiveness of said claims, as argued in the former Written Opinion, still has to be maintained.

A METHOD OF AND APPARATUS FOR GENERATION OF A KEY

FIELD OF THE INVENTION

The present invention relates to the field of data, device and communication protection and access control and in particular to a method of and apparatus for generation of a key.

BACKGROUND OF THE INVENTION

It is often necessary to protect data in digital form that is stored in data storage devices and/or transmitted over a network. To prevent un-authorized access of the data, encryption techniques are widely used. Essential problems of existing encryption techniques are (1) where to keep the encryption key, so that it remains safe and (2) how to authenticate a user in the most effective way. Currently, passwords and access cards or tokens are widely used for authentication. A password, however, can be easily attacked, and access cards can be easily lost. A user may lose valuable data forever if the password or card is forgotten or lost.

In order to address this problem, techniques have been proposed based on the use of biometrics of a user, that is to say, physical characteristics of the user that identify the user unambiguously. In several prior art proposals

such biometrics data is used to gain access to a computer system. The biometrics data is stored on a token for future reference. When the user subsequently wishes to obtain access to the system, the identity of the user is verified by comparing the biometrics data of the user with that stored on the token. These proposals have the disadvantage that a token is required, which may be lost or compromised. In U.S. 5613012, a tokenless identification system is disclosed based on a correlative comparison of a unique biometrics sample, such as a fingerprint or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.

These proposals have the disadvantage that an assumption is made that the storage devices are secure and that a secure communication link with the device is established. It is not true in many cases. In a networked environment, client devices can be public. Although the authorization data may be kept in a very secure place in the authenticating computer system, analogous to a safe deposit box in a bank, such data may still be accessible by the system operators and thus the data is not completely secure.

It is an object of the invention to provide a method of protecting digital data which alleviates this disadvantage of the prior art.

SUMMARY OF THE INVENTION

According to the invention, there is provided a method of generating a key or set of keys from a person's biometrics data comprising the steps of:

(1) capturing the person's biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant feature measures from the normalized data and representing the feature measures as a bit pattern;

(4) storing the bit pattern in associative memory in an enrolment / registration phase and recalling the stored bit pattern from the associative memory in an identification / verification phase; and

(5) generating the key from the recalled bit pattern.

According to the invention in a second aspect, there is provided a method of generating a representation of biometrics data comprising the steps of:

(1) capturing the biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern.

According to the invention in a third aspect, there is provided a method of controlling access by generation of an access key from a person's biometrics data comprising the steps of:

(1) capturing the person's biometrics data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as an initial bit pattern;

(4) storing the initial bit pattern in associative memory for retrieval;

(5) repeating steps (1)-(3) at a subsequent time to generate a subsequent bit pattern;

(6) inputting the subsequent bit pattern to the associative memory to recall the stored bit pattern; and

(7) generating the key from the recalled bit pattern.

According to the invention in a fourth aspect, there is provided a method of generating a key from the person's biometrics data which comprises the steps of:

(1) capturing the person's biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern;

(4) storing the bit pattern in associative memory for retrieval;and

(5) generating the key from the retrieved bit pattern.

The invention further comprises apparatus for performing any of the above methods.

According to the invention in a fifth aspect, there is provided a codebook to store data from which, upon

retrieval, a key is generated, the codebook comprising distributed associative memory.

The embodiment described is a tamper-resistant method and system to generate a unique key from biometrics of a person, using neural network associative memory. The captured biometrics data of a person may vary from time to time for reasons such as variation of the biometrics itself and variation of capturing conditions. The method compensates for this by first detecting invariant features from the biometrics. These features form feature measures in the format of a bit pattern which is stored in associative memory. At the authentication phase, the biometrics data is captured again from the user and the feature measures are again generated. The resulting bit pattern is then used to recall the bit pattern previously stored in the associative memory, which is unique to the user. A unique key can then be generated from the recalled pattern. Since associative memory is highly parallel and distributed, it is practically impossible to find exact patterns stored in the memory. Only a valid biometrics feature pattern can recall a valid stored pattern and generate a valid key for encryption and other purposes, such as for security, identity verification, as a PIN number or as a password.

The key may be of any kind, for example a public/private key pair, identity key or symmetry key.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a flow chart of the algorithm of an embodiment of the present invention.

Figure 2 illustrates the functions of parallel distributed associative memory in the embodiment of Figure 1.

Figure 3 illustrates feature points of a finger print.

Figure 4 illustrates a variation of the embodiment of the present invention in which multiple biometrics are combined for key generation.

Figure 5 illustrates another variation of the embodiment of the present invention using multiple associative memory codebooks.

DETAILED DESCRIPTION OF THE DESCRIBED EMBODIMENT

An embodiment of the method and apparatus to generate a unique private key for encryption / decryption, or a key for a digital lock, for secure communication, access control, ownership claiming and other applications will now

be described. In the following description, the overall flow chart of the system is first explained, followed by a detailed description of each step of the system. In this description, use of fingerprint and face (appearance) biometrics data will be used as examples, although it will be understood that the method is equally applicable for use with other biometrics data such as, but not limited to, hand geometry, hand vein, iris, retinal pattern, signature, voice print and facial thermograms. There will be differences in the initial step to convert the biometrics data into feature measures in the format of a bit pattern, but once the biometrics data has been converted into such feature measures, all other processing steps will be exactly the same for all types of biometrics.

As shown in Figure 1, the method has the following basic steps:

Biometrics data acquisition (1): In this step, acquisition devices such as a finger print scanner / sensor are used to capture image data or other forms of biometrics data.

Normalization of biometrics data (2): In this step, the data of Step 1 is processed in order to reduce the effect of variations due to capturing condition changes. Such processing includes scale change, translation, rotation, and lighting and background changes.

Feature encoding (3): In this step, feature measures which represent the invariant features of the biometrics are extracted and a bit pattern is generated from the feature measures.

Feature Registration and Matching (4): In this step the feature measure bit pattern is processed by a codebook 4a implemented as distributed associative memory. In an enrolment and registration step 4b, the bit pattern stored into the associative memory by learning. In a subsequent matching/recognition step 4c, a subsequently generated bit pattern is used to recall the bit pattern previously stored in the codebook to provide an activated pattern at step 4d.

Key Generation (5): In this step, a key is generated from the activated pattern. In case of enrolment/registration, the generated key is registered with the relevant authority or used to lock or encrypt the items to be protected. In case of matching/recognition, the generated key is used to unlock or decrypt the items protected, or to authorize the person.

The techniques used in the each step will now be described:

1.   Biometrics data acquisition

The technique employed for acquiring the biometrics data

depends on the biometrics used. In this description, fingerprint and face biometrics data are used as examples of the method. For fingerprints, either of the two primary techniques, i.e. inked or live scan may be used. With the inked method, an inked fingerprint image is taken and this is scanned into a computer. In the live scan technique, the fingerprint image is obtained by the scanner directly. For face, a digital picture of the face is obtained either through scanning of a photograph or directly with a digital camera. For both kinds of biometrics, biometrics data in the form of a digital image is obtained.

For additional authentication, it is desirable to capture live biometrics data, that is, the capture device must be able to verify that the biometrics data captured is from a live person. This can be done by by employing various techniques for various biometrics. For face recognition, where the video camera continuously captures a face image with a speed, for example of 30 frames per second, a processing function to check for motion of the face and facial expressions may be employed. If both face motion and facial expressions are regular, the face images captured are "live". They will be rejected as false otherwise. There are, similarly, scanners available which make use of the properties of a "live" fingerprint. In the case of speaker identification, the aquisition system can prompt the speaker to repeat a voice segment (eg a phrase or name) several times and check for variations, the

absence of which between any two segments will cause the
biometrics data to be rejected.

2.   Normalization of biometrics data

Normalisation in general is a common concept in image
processing and is discussed, for example in A. Rosenfield,
A. C. Kak, Digital image processing, Academic Press, New
York, Second edition, 1982.

In the described embodiment, the biometrics data is
normalised with reference to landmarks, which are central
to the data and exist for all circumstances. The
normalization is then done using these landmarks. By
normalization is meant scaling the data range to a standard
range and transforming the biometrics image to a standard
location, orientation, and scale. The typical normalization
methods for fingerprint and face biometrics data are well
known in the art and examples are as follows:

Finger print: Filtering to enhance minutiae points,
identification of the core (a small but consistent part of
the finger) and use of the core location and orientation to
define a geometric transform for normalization.

Face: Identify the face region and eyes, use the location
of two eyes to define a geometric transform. Focus on face
region and perform histogram normalization to reduce the

effect of background and lighting condition changes and transform the face image using the defined geometric transform.

3.   **Invariant feature extraction**

In this step, a bit pattern is generated to represent the invariant features of the biometrics of a person. The bit pattern is not a binary version of the actual biometrics image but is formed by using salient feature points and possible lines linking those feature points. Figure 3 shows an example of feature points used to generate a bit pattern of a finger print. Here, salient feature points are highlighted with black points linked by the lines shown. Since invariant salient feature points are extracted from the normalized image, for the same person, the locations of those feature points would be almost the same. For fingerprint biometrics data, minutiae points of fingerprints are used as feature points. In the case of face biometrics, feature points such as the corners detected by Harris and Stephens (Harris, C. and Stephens, M. (1988) A combined corner and edge detector, Proc. 4th Alvey Vision Conference, pp 147-151) are invariant and can be used to form the bit pattern.

Feature points are of varying importance and a representation scheme for the bit pattern generation may be used. For example, in a fingerprint image, minutiae points

are considered more important than ridge points, so more (data) bits can be assigned to represent the minutiae points in the bit pattern.

The data forming the bit patterns may represent feature points from a smaller area than the original biometrics image with the central part emphasized, since parts far from central part may be missing in some cases.

4.   Associative memory codebook and its operations

Associative memory codebooks can be implemented using various neural networks provided the stored patterns are randomly distributed. Hopfield-like networks are one of the possible implementations and will be used to explain this part of the described embodiment of the invention.

Supposing that the bit pattern extracted from the original biometrics image has size of M by N, then, there should be MN nodes in the Hopfield network. The network is fully connected. A node receives input from all other nodes. There is no distinction between input nodes, hidden nodes and output nodes. The total energy function of the network system is defined as summation of productions of value of all possible pairs of nodes and the link weight between them. The energy minima are referred to as stable states. The network stores information via its stable points in the

state space. The state evolution of the network system performs a gradient descent toward energy minima, and always ends up in a state of equilibrium. When the system reaches equilibrium, no state changes will happen to any node of the neural network system.

The bit patterns are stored by learning. One or several bit patterns representing the biometrics of a person are presented to the network as input and the network will evolve to create a stable state corresponding to the input patterns.

The information retrieval is performed by state evolution. When a subsequent input bit pattern is presented, all nodes obtain their initial state from the input bit pattern. The information is retrieved when the state evolution reaches a local stable point. The retrieved (activated) pattern is represented by states of MN nodes as a binary word of MN bits.

Figure 2 illustrates the functions provided by the associative memory which plays the roles of both matching/recognition (10) and biometrics database (12) of prior art methods. It is also coupled with the decision making (14) and key generation (16)/rejection (18) process in the sense that tolerance of distortion of the recalled bit pattern is reflected in the key generation, and that the key is directly generated from the recalled bit pattern

while in the prior art, the key is assigned using separated methods. By doing so, the method of the described embodiment successfully hides the biometrics database and the key generation methods, making them difficult to attack.

The key to be generated, which can be used as a public/private key pair and/or an identity key, requires more than 128 bits for security reasons. In the present method, the coordinates of salient points (around 48) are used to generate the private key, which can be as long as 48 x 2 bytes = 768 bits.

Using a Hopfield-like neural network as associative memory, for any given input pattern, the network evolution will converge to a stable state. The tamper resistance of the present method can best be explained in answer to the following question: if an attacker randomly input a biometrics pattern, what is the probability that the network converges to a stored valid biometrics pattern? This can be looked at in three ways:

1. Using the method of *steepest descent* or *Saddle-point approximation* (for example, as disclosed in the book "Neural Networks" by B. Muller J. Reinhardt, Springer-Verlag) it can be shown that in addition to the minima which correspond to the stored patterns, there are $\frac{1}{2}3^p$

spurious stable states for p < N, where p is the number of stored patterns. For a valid input pattern, there is no problem to converge to the corresponding minima since the starting point is very near the minima. But for a random input pattern, the probability of converging to a minima representing a valid biometrics patterns is very low: $2p3^{-p}$. Assume that there are 128 stored patterns, this probability will be much less than 2^{-128}, the attack probability for a 128 bit key. In the case of very few users, one can choose to store more (more than 128) patterns and only validate the few users.

2.   When searching for a stored pattern with an input pattern by searching for minima of the energy function, the energy function actually represents the correlation between the input pattern and the stored pattern. As it is known that the correlation function usually does not have a sharp peak and noise exists, in practice, the recalled pattern is a mixture of the input pattern and the stored pattern (see book "Neural Networks and Simulation Methods" by Jian Kang WU, Marcel Dekker Inc.). The generated key will not be a valid one if the input pattern is quite different from the recalled one. That is to say, the input pattern must resemble the stored valid pattern in order to generate a valid key. By the nature of biometrics, there should not be any two identical biometrics patterns. That means that attacker must

randomly generate biometrics patterns which resemble the valid ones (at least, with certain degree of similarity). Assume that each pattern is characterized by 48 salient feature points and that the image size is 512 × 512, 18 bits are needed to code the coordinates of those points. To allow for 4 pixels variation of feature points, the 18 bits are reduced to 12 bits for coordinate coding. There are all together 48 × 12 = 576 bits to code a pattern. Since there are p valid stored patterns, the probability of resembling a valid pattern will be $p2^{-576}$

3.   The storage capacity of Hopfield network can be as high as 2N even for non-orthogonal patterns using the learning method by Krauth and Mezard (See "Neural Networks" by B. Muller, J. Reinhardt; Springer-Verlag). To improve further the tamper-resistance of the system, a portion of the stored biometrics patterns can be validated. For a typical network size of 400 × 500, N=200,000. Within 400,000 stored patterns, only 400 patterns are validated. This further improves the tamper-resistance by reducing the attack probability by 1/1000.

5.   **Key Generation**

In either the enrolment/registration (storage of bit pattern to associative memory) phase or the matching / recognition (pattern retrieval from associative memory)

phase, there is a stable state reached by network evolution. The states of nodes at the stable state represent the valid bit pattern of biometrics of a person. A unique key can be generated from the pattern.

Since there may be noise in the storage and retrieval process of the associative memory, it is preferred not to use directly the whole bit pattern represented by the network stable state to generate keys. Rather, only the most reliable and important feature points in the bit pattern are used. To decide on these points, a person to be enrolled in the enrolment/registration phase will repeat the step (1) of having his/her biometrics data captured as samples. The reliable feature points are defined as those points persistent for all sample biometrics data collected in the enrolment/registration phase.

When the important feature points are identified from the bit pattern, a hash algorithm (see book: Bruce Schneider, Applied Cryptography: protocols, algorithms and source code in C; John Wiley & Sons 1996) can be used to generate a unique key, that may be further used to generate the private key and public key for a specific application, such keys then being used to encrypt and decrypt data as this is input and output.

For some applications, the key needs to be changed within a certain period. This can be achieved by adding and

changing at least one parameter in the key generation program.

To achieve higher security, multiple biometrics can be combined for authentication. For example, using multiple finger prints, a combination of finger print with voice, etc. This is illustrated in Fig. 4 in which one set of processing modules 3-4d ...4d' ...4d" (capturing, normalisation, feature extraction and encoding, and registration/recall of associative memory codebook) for each biometrics is necessary to obtain recalled/activated pattern. All recalled/activated patterns (1, 2, ...,n) are then input to key generation module, and combined to generate one key.

In case of multiple data items of the same type of biometrics, for example, multiple finger prints, finger print data (1, 2, ...,n) are processed using one set of processing modules to obtain activated patterns for respective finger prints. When all recalled patterns arrive at the key generation module, a key is generated using all of recalled patterns.

If it is assumed that two finger prints are combined for authentication, since the false acceptance rate (FAR) for a finger print is 10^{-4}, combining two will result in FAR of 10^{-8}.

In case of large users, one associative memory may not be able to store all biometrics patterns. In such a case, multiple parallel associative memories 4a, 4a', 4a" and 4a'" can be used as illustrated in Fig. 5. Since such memories will run in parallel, the speed of authentication will not be reduced.

The method of the present invention can be implemented with a digital processor for example an ordinary computer, suitably programmed.

CLAIMS:

1.   A method of generating a key or set of keys from a person's biometrics data comprising the steps of:

(1)   capturing the person's biometric data;

(2)   normalizing the captured biometrics data,

(3)   extracting invariant feature measures from the normalized data and representing the feature measures as a bit pattern;

(4)   storing the bit pattern in associative memory in an enrolment / registration phase and recalling the stored bit pattern from the associative memory in an identification / verification phase; and

(5)   generating the key from the recalled bit pattern.

2.   A method as claimed in Claim 1 wherein the normalization step includes the step of selecting reference points of the captured biometrics data and normalizing the data with respect to the reference points.

3.   A method as claimed in Claim 2 wherein the biometrics data comprises a face image and the reference points comprise the location of the eye portions of the face image.

4.   A method as claimed in Claim 2 wherein the biometrics data comprises a fingerprint image and the reference points comprise the location and orientation of

the core of the fingerprint image.

5.   A method as claimed in any one of the preceding
Claims wherein the biometrics data comprises an image and
the features are selected from normalized data
corresponding to a portion of the image.

6.   A method as claimed in any one of the preceding
Claims wherein the bit pattern is generated from the
features using a representation scheme.

7.   A method as claimed in Claim 6 wherein the features
are represented according to importance.

8.   A method as claimed in any one of the preceding
Claims wherein the image is a fingerprint image and the
feature measures are of minutiae points.

9.   A method as claimed in any one of Claims 1 to 7
wherein the image is a face image and the feature
measures are of corners of the image.

10.   A method as claimed in any one of the preceding
Claims wherein the associative memory is implemented
using a neural network.

11.   A method as claimed in claim 10 wherein the neural
network is a Hopfield network.

12. A method as claimed in any one of the preceding claims wherein, in step (5), a symmetry key or public/private key pair is generated.

13. A method as claimed in claim 12 further comprising the step of performing encryption or decryption using the key when inputting or outputting data.

14. A method as claimed in any one of the preceding Claims wherein steps (1)-(4) are applied to a plurality of biometrics data sources, the key being generated from a respective plurality of retrieved bit patterns.

15. A method as claimed in Claim 14 wherein the biometrics data sources are of different types.

16. A method as claimed in any one of the preceding Claims wherein a plurality of keys corresponding to a plurality of persons are generated and the corresponding bit patterns are stored in two or more parallel associative memories.

17. A method as claimed in any one of the preceding Claims wherein step (1) is performed a plurality of times to provide a plurality of samples and only invariant feature measures persistent in all samples are used to generate the key.

18. A method of generating a representation of a biometrics image comprising the steps of:

(1) capturing the biometric image;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern.

19. A method as claimed in Claim 18 wherein the features are selected from normalized data corresponding to a portion of the image.

20. A method as claimed Claim 18 or Claim 19 wherein the bit pattern is generated from the features using a representation scheme.

21. A method as claimed in Claim 20 wherein the features are represented according to importance.

22. A method of controlling access by generation of an access key from a person's biometrics data comprising the steps of:

(1) capturing the person's biometrics data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as an initial bit pattern;

(4) storing the initial bit pattern in associative memory for retrieval;

(5) repeating steps (1)-(3) at a subsequent time to generate a subsequent bit pattern;

(6) inputting the subsequent bit pattern to the associative memory to recall the stored bit pattern; and

(7) generating the key from the recalled bit pattern.

23. A method of generating a key from the person's biometrics data which comprises the steps of:

(1) capturing the person's biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern;

(4) storing the bit pattern in associative memory for retrieval;and

(5) generating the key from the retrieved bit pattern.

24. Apparatus for performing the method of any one of Claims 1-23.

25. Apparatus as claimed in claim 24 being a digital processor programmed to perform the method.

26. Apparatus as claimed in claim 24 or claim 25 including a biometrics capturing device.

27. Apparatus as claimed in claim 26 wherein the device captures live biometrics data.

28.   A codebook to store data from which, upon retrieval,
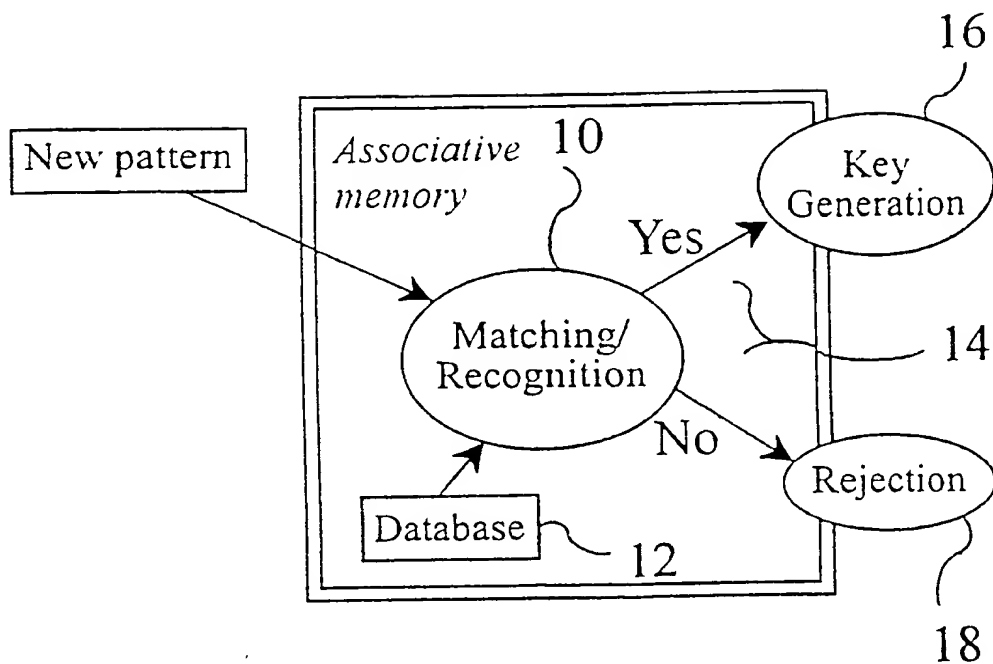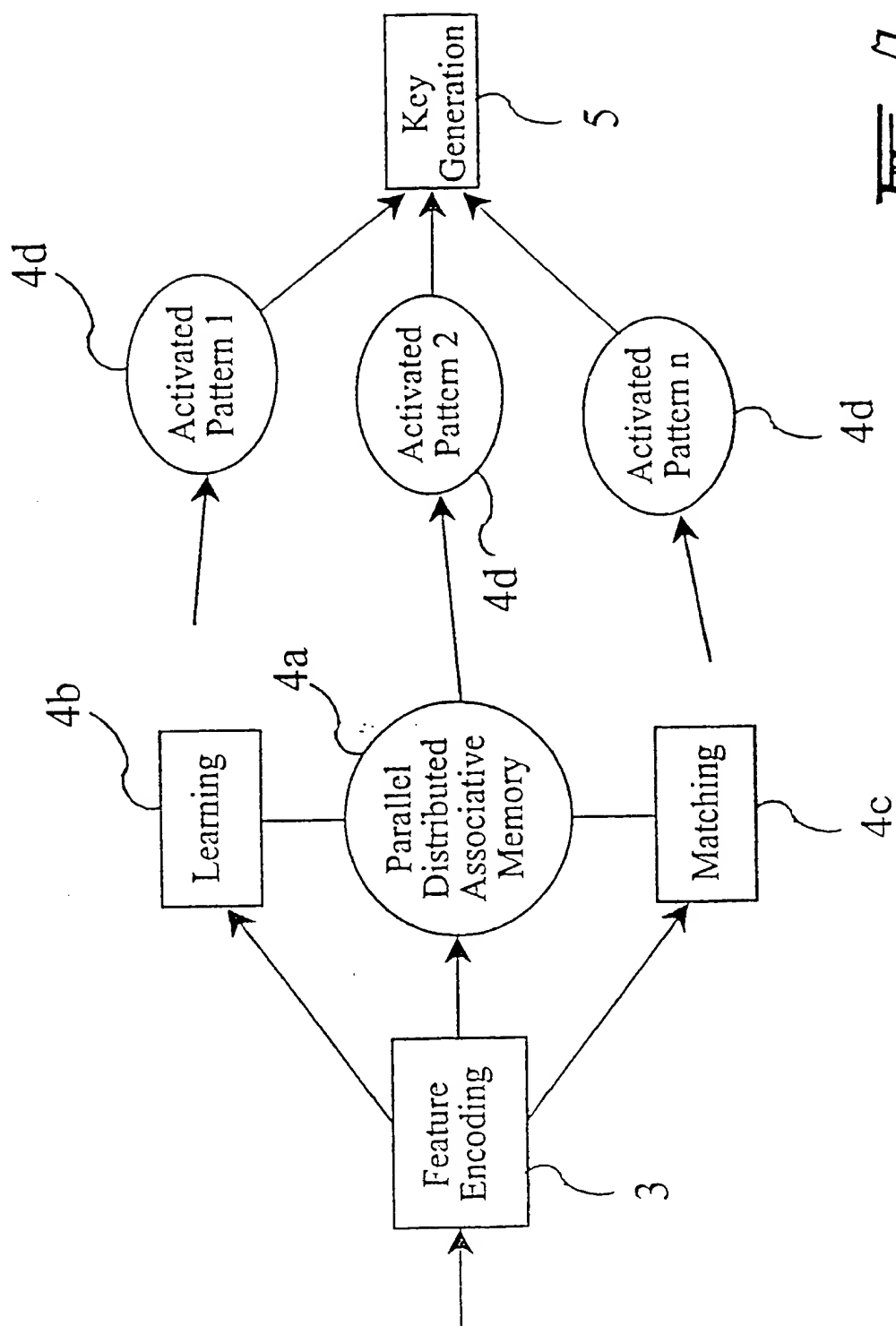a key is generated, the codebook comprising distributed
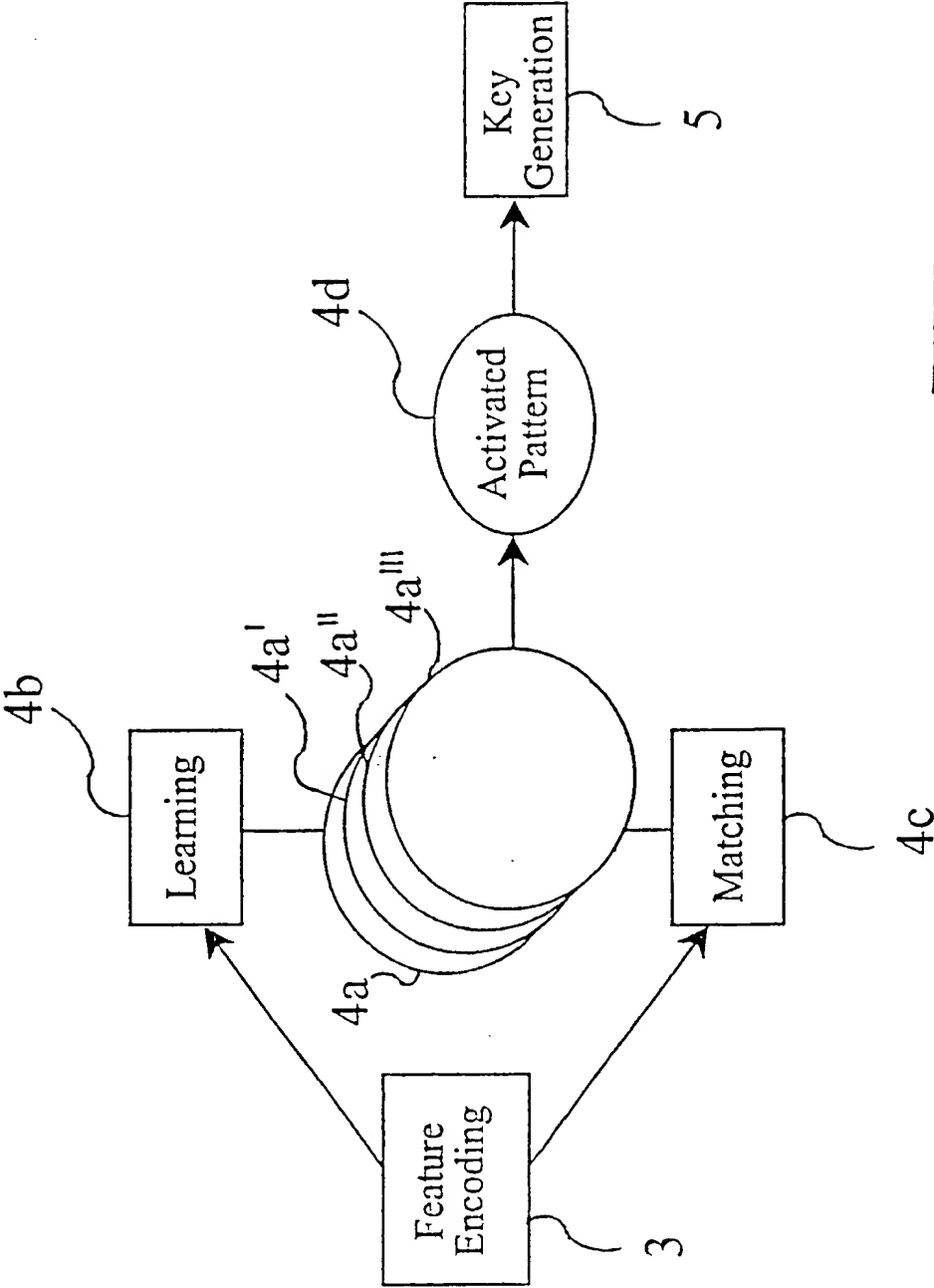associative memory.

FIG. 1.

$\overline{I\!I\!I}\_2.$

$\overline{I\!I\!I}\_3.$

FIG. 4.
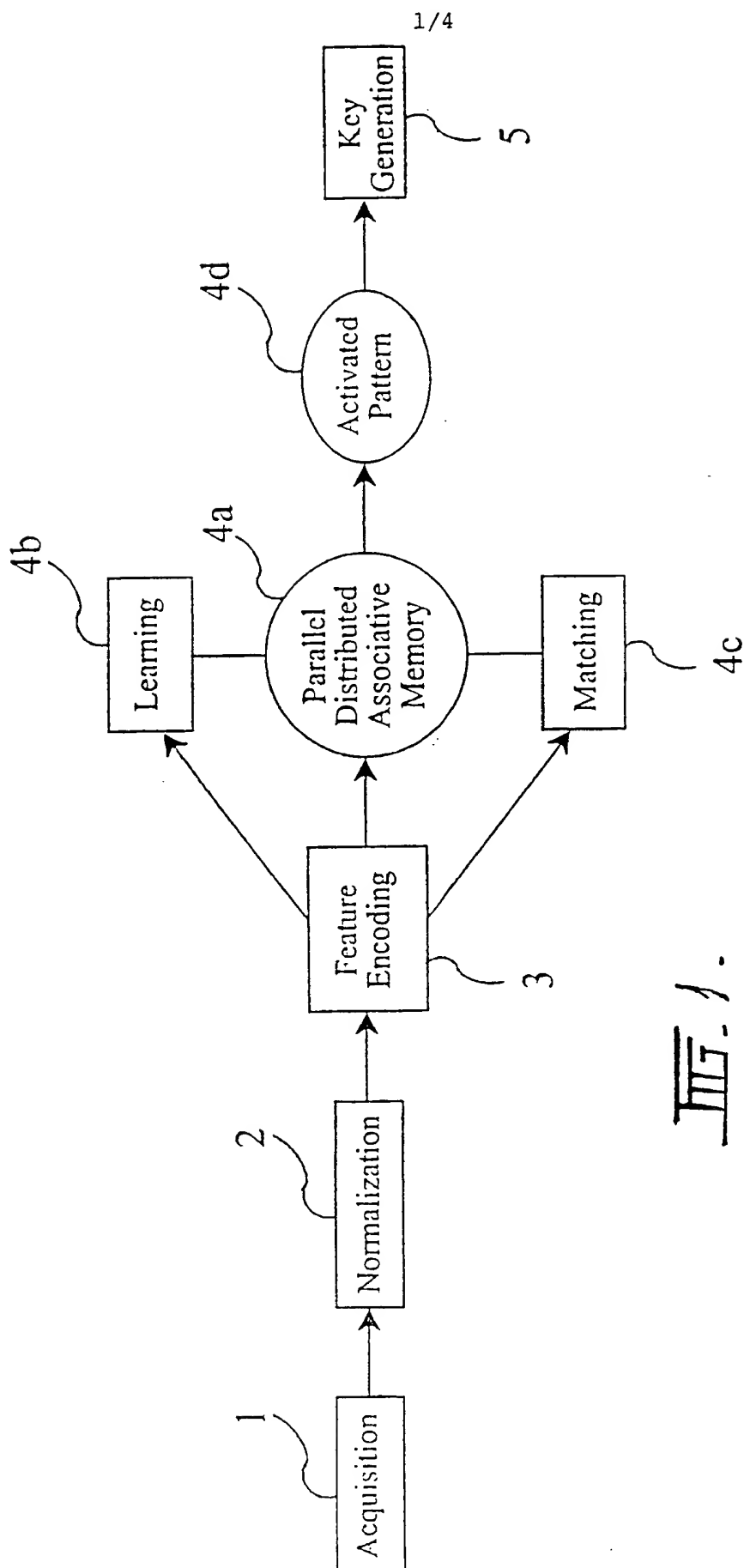
Fig. 5.

INTERNATIONAL SEARCH REPORT

	International application No.
	PCT/SG 98/00067

A. CLASSIFICATION OF SUBJECT MATTER

IPC⁶: G 09 K 9/00, G 07 C 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC⁶: G 09 K, G 07 C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

G 06 F, H 04 L

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 42 43 908 A1 (GAO) 30 June 1994 (30.06.94), totality.	1,2,4-8,12-17,18-27
Y		3,9-11
X	WO 96/08 093 A1 (MYTEC TECH.) 14 March 1996 (14.03.96), page 3, lines 1-19; claims.	1,2,4-8,12-17,18-27
Y	US 5 497 430 A (SADOVNIK) 05 March 1996 (05.03.96), abstract; claims.	3,9-11

☐ Further documents are listed in the continuation of Box C.   ☒ See patent family annex.

Date of the actual completion of the international search	Date of mailing of the international search report
06 April 1999 (06.04.99)	04 June 1999 (04.06.99)

Name and mailing adress of the ISA/AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna	Schlechter
Facsimile No. 1/53424/535	Telephone No. 1/53424/448

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

| Box I | Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet) |

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
   because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
   because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
   because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

| Box II | Observations where unity of invention is lacking (Continuation of item 2 of first sheet) |

This International Searching Authority found multiple inventions in this international application, as follows:

```
Claims 1-27:  Method of generating a key and/or access control from a person's
              biometric data

Claim 28:     Codebook for storing data
```

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest   ☐ The additional search fees were accompanied by the applicant's protest.

                     ☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
DE A1 4243908	30-06-1994	keine - none - rien	
WO A1 9608093	14-03-1996	AU A1 33390/95	27-03-1996
		AU B2 689946	09-04-1998
		BR A 9509002	02-06-1998
		CA AA 2199034	14-03-1996
		CN A 1157677	20-08-1997
		EP A2 780040	25-06-1997
		JP T2 10505474	26-05-1998
		US A 5680460	21-10-1997
		US A 5541994	30-07-1996
		US A 5832091	03-11-1998
		US A 5737420	07-04-1998
		AU A1 47109/96	26-02-1997
		US A 5712912	27-01-1998
		WO A1 9705578	13-02-1997
		AU A1 10895/97	01-08-1997
		WO A1 9725800	17-07-1997
US A 5497430	05-03-1996	keine - none - rien	